All That Glitters Isn't Gold

by Steve Brown

We recently read about the plight of a Florida woman who lost her eye and nearly died after a single piece of glitter from a Valentine's Day card became lodged in her eye and caused a raging, life-threatening infection. Try as they could, doctors weren't able to save the woman's eye, though she did narrowly escape with her life. The grateful mother of two is now using her ordeal as a cautionary tale, urging parents working with glitter to wear proper eye protection.

Similarly, when it comes to protecting a bank and its customers against fraud, there's no such thing as being too careful. Certainly, as fraud losses are mounting from multiple angles, it's even more incumbent on banks to hone in on even the smallest things that may seem amiss.

One particular area of concern is the dramatic increase in so-called "CEO fraud," which we've touched on before, but bears repeat emphasis. These are e-mail scams in which hackers masquerade as a CEO or other executive and send emails from a spoofed account. Those emails tell employees to send wires out (usually the CFO) for a late payment of some sort. The messages look legitimate and many businesses and banks alike may not realize there's a problem until it's too late.

The FBI indicates it has seen a 270% jump in victims and losses due to business email compromise just like this. Indeed, from Oct 2013 to Feb 2016, there have been 17,642 victims and $2.3B in losses reported, according to the FBI. One takeaway for banks is to redouble efforts around all requests for money before initiating any transactions. Extra steps can make all the difference between large losses and stopping attackers in their tracks.

Another area of concern is ACH fraud. After all, with some 25B ACH transactions flowing through this pipe, it is gleaming pile of money glitter to the eyes of hackers and criminals. Further, the more business customers and banks do things over the internet the more ACH likely comes into play and all of the bad actors that follow it. Key areas that experts say bankers should know about include such things as stealing a password and pretending to be a customer or setting up fake charities (or other companies) that steal an increasing amount of money each day. Those amounts are then returned as an ACH credit the next day and a larger amount is then debited the next day and so on. This process slowly builds the net exposure over time and eventually millions of dollars are stolen when all is said and done.

In the ACH world, crooks are so sophisticated, that in some instances they will even edit items within a batch itself so the money is stolen but the batch total itself remains the same. This clever workaround is just one way thieves avoid countermeasure software banks may use. Keystroke logging malware is the primary way such thefts occur and then false entries are created to abscond with money. Several banks have been hit on this one.

Once hackers have access to employee or customer IDs and passwords, or account numbers and other sensitive information, they can cause all sorts of havoc but appear to be legitimate.

Keyloggers are hard to detect, which is why many IT teams do not allow employees to download software to their work computers. Even a small step such as this can go a long way in protecting your bank.

Even everyday transactions need to be looked at with a careful eye to make sure everything is copasetic. If banks don't employ the proper intelligence systems and train employees to recognize fraud warning signs, great losses can occur in the blink of an eye. When it comes to fraud in banking, as the saying goes - "all that glitters is not gold," so be alert and keep training your staff.

BANK NEWS

Website Options

A survey of small businesses by Wasp Barcode Technologies finds the following options and services offered on business websites: learn about goods or services offered (62%); get company locations, phone numbers and email (51%); contact sales or customer service (49%); apply for a job (35%); watch videos (35%); get social media links (34%); schedule appointments or register for events (33%); buy goods and services offered (32%); learn about employees (29%); read the company blog (28%); and do not have a website (6%).

Borrowing Source

Research by the EBRI on retirement finds 23% of workers have taken out a loan against their retirement savings plan. Reasons cited are: pay off debt (21%); purchase home (17%); home improvement (13%); health problem or disability (13%); family situation (10%); not working (9%); purchase a car (6%); and education expenses (5%).

Single Security

The FHFA is working to create a single security this year that will bring together FNMA and FHLMC mortgage backed securities. The shift will streamline the process and reduce costs associated with creating and administering such MBS.

Lending Growth

A survey of financial professionals by the AFP finds the factors that would lead companies to deploy their excess cash are: stronger domestic economic environment (46%); improvements in customer demand (44%); stronger global environment (29%); greater financial markets stability or predictability (27%); and reduced regulatory burdens and uncertainty (24%).